IMPLEMENTACION DE UN SISTEMA DE CONTROL INTERNO EN UN CENTRO DE PROCESAMIENTO DE DATOS

Carlos A. Petrella
Ministerio de Transporte y Obras Públicas
Montevideo - URUGUAY

RESUMEN:

El estudio plantea los principales problemas derivados del desarrollo de un Sistema de Control Interno en un Centro de Procesamiento de Datos, describiendo las distintas etapas que se cumplen para implantarlo.

Primero, se plantean problemas de capacitación del personal y las necesidades prácticas de ajustes organizativos; luego, el énfasis se traslada a los problemas derivados de la falta de continuidad del servicio, para proyectarse a continuación sobre el control de costos operativos y nivel de servicio y por último, hacer hincapié en la planificación como factor importante para impulsar el desarrollo de los sistemas de información.

La base de la estrategia propuesta para encarar la implantación del sistema tiene como objetivo crear una adecuada conciencia de la magnitud de los problemas derivados de la falta de control, buscando ganar la colaboración del personal en todos los niveles a través de procedimientos que establezcan objetivos comunes, identifiquen riesgos, definan áreas de responsabilidad individuales y utilicen estos resultados para medir la contribución de cada empleado al cumplimiento de los objetivos corporativos.

El estudio recoge planteos teóricos y experiencias prácticas de varios paises latinoamericanos, analizando propuestas, para solucionar los principales problemas que se enfrentan al desarrollar controles en los sistemas de procesamiento automático de datos.

PLANTEO DEL PROBLEMA

Uno de los principales problemas que enfrentaremos al desarrollar controles es el derivado de que en el pasado, los criterios de diseño de procedimientos de control sobre los sistemas informáticos han puesto énfasis sobre aspectos tecnológicos postergando la consideración de aspectos vinculados con la organización, su personal y la propia gestión de administración de los recursos. (Referencia: System Auditability and Control, (Control Practices Report) Preparado por The Institute of Internal Auditors, Inc.).

Es más, la definición de sistemas de procesamiento de datos (SPD) suele aplicarse en forma restringida limitándola exclusivamente a los equipos electrónicos y su software asociado. Sin embargo, un SPD incluye además otros componentes: personal, materiales y procedimientos que actúan sobre la materia prima (datos) para obtener el producto elaborado (información). Por supuesto, objetivamente no puede dudarse de la importancia de cualquiera de ellos, sin embargo frecuentemente se responsabiliza en forma genérica a la computadora de la mayoría de los incidentes que ocurren en torno a un SPD. Es más, quien no ha escuchado alguna vez "el computador se equivocó" sin que el acusador vislumbre sombras de sospechas de fallas en el entorno del mismo. Evidentemente los problemas de funcionamiento del sistema pueden deberse directa o indirectamente a cualquiera de sus componentes. A su vez estos componentes están muy interrelacionados, razón por la cual por ejemplo, una falla en los procedimientos repercute en la calidad del producto terminado tan fuertemente como un error de lógica en un programa, o un incidente en la operación del computador.

Así pues todo el sistema debe disponer de filtros de control de calidad en cada paso de la cadena de producción hasta la obtención del resultado deseado. El problema reside en que, a pesar de que existe concenso respecto a que los filtros son necesarios, los sistemas mecanizados suelen prescindir peligrosamente de ellos.

La desinformación lleva a diseñar sistemas sin los debidos controles y requisitos de auditoría que luego hacen muy dificultosa la evaluación de su funcionamiento.

¿Que pensaría un gerente bancario si se pagara un cheque sin control de saldos y sin autorización previa? Seguramente se alarmaría y realizaría una investigación del hecho tratando de determinar responsabilidades. Sin embargo como contrapartida,

¿qué controles se exigen sobre el acceso a los recursos, y la protección de registros, los procedimientos de recuperación y resguardo sobre los archivos de cuentas corrientes una vez mecanizados? Obviamente la indiferencia para evaluar el funcionamiento de un sistema mecanizado es solamente producto del desconocimiento de su impacto sobre la organización por parte de usuarios y especialistas.

Ante este panorama, queda claro que, debería haber siempre un vínculo estrecho entre las funciones de control interno y procesamiento de datos, no solamente a nivel de la organización de la unidad encargada de procesamiento, sino, a nivel de los sistemas de información que usan procesamiento electrónico de datos. Es más, los propios sistemas de información deberían ser considerados parte del activo de la organización y custodiados con tanto esmero como las mismas cuentas bancarias (Referencia: El control interno sobre un sistema automático de procesamiento de datos del autor).

LA IMPLANTACION DE UN SISTEMA DE CONTROL INTERNO

El enfoque planteado refuerza la idea de que la instalación de un sistema de control interno es un proceso dinámico que involucra a todos los integrantes de la organización y cuya cooperación es imprescindible para mejorar el comportamiento de los sistemas de información. Como consecuencia del caracter dinámico de los sistemas, el proceso de implantación de un sistema de control interno se va desarrollando ciclicamente y en cada ciclo se diferencian períodos: relevamiento, elaboración de una propuesta, implantación y evaluación.

Cada ciclo se inicia con un relevamiento para reconocer problemas que directa o indirectamente afectan la calidad del servicio. Luego se intentan aplicar estandares correctivos con el objetivo de normalizar el funcionamiento del área afectada. Posteriormente se definen mecanismos para controlar el proceso verificando los resultados, buscando eficacia primero, y eficiencia después. Por último sobre la base de la información recogida, se inicia un nuevo ciclo.

Una vez cumplido cada ciclo se retro-alimenta el sistema lográndose un más eficiente reconocimiento de problemas que provocan nuevos ajustes que mejorarán aun más el sistema.

A su vez como las necesidades de la organización van cambiando en cada ciclo (relevamiento, propuesta, implantación y evaluación) variarán los objetivos de acuerdo con su grado de evolución. En ese sentido, se podrían diferenciar etapas en la evolución en los sistemas de información y los Centros de

Procesamiento de Datos (CPD) que van desde la prácticamente inexistencia de controles hasta la madurez institucional y que aportan gradualmente garantías crecientes. La primera etapa, pone énfasis en la capacitación y los ajustes organizativos, pasando luego, en una segunda etapa, por los esfuerzos vinculados con el mantenimiento de la continuidad del servicio, para hacer después incapié en el nivel de servicio y el control de los costos operativos y proyectarse al final, en la cuarta etapa, sobre tareas de planificación, estructurando planes de desarrollo viables y no expresiones de deseo que no siempre pueden ponerse en práctica. Así pues, las etapas que se identifican en la evolución hacia la madurez son las siguientes:

1) La capacitación y los ajustes organizativos (búsqueda)
2) La continuidad del servicio (seguridad)
3) Los costos operativos y los niveles de servicio (control)
4) La planificación (desarrollo)

La definición de estas etapas no implica que por ejemplo, si el énfasis en un período está puesto en la continuidad del servicio no exista interés por abaratar costos de operación o no haya preocupación por la queja de los usuarios ante un nivel del servicio que consideran inadecuado.

A continuación, se detallan las características de cada etapa y las principales actividades que se derivan de las metas planteadas a cada nivel de la evolución.

ETAPA 1 BUSQUEDA

La primer etapa, al igual que al nacer un ser humano, es de descubrimientos, y apunta al conocimiento de sus propias posibilidades y la adaptación al ambiente.

Así, pues, el trabajo comienza por los ajustes en la organización. Cuando se busca realizar ajustes organizativos con vistas a mejorar los sistemas de control interno, la participación de todos los integrantes de la organización y en particular de los especialistas de su CPD es fundamental. El personal debe ser involucrado desde el comienzo del proceso de tal manera de que no sienta que los controles se le imponen sino que deben ser implantados para salvaguardar su propia fuente de trabajo y, más generalmente, los objetivos de la empresa protegiendo sus áreas críticas.

Una forma de involucrar al personal es enfrentarlo con los riesgos que cada uno individualmente asume al no disponerse de sistemas de protección y control.

A su vez, para que cada uno, en la medida de sus posibilidades, aporte soluciones a los problemas, debería brindarse un curso inicial sobre organización y control interno de los sistemas de información y más específicamente, para algunos de ellos, de la propia "cocina" de los sistemas: su CPD. Estos cursos deberían permitir introducir a los usuarios en el mundo informático y acercar a los especialistas al mundo empresarial para que de ambas vertientes se obtenga un diagnóstico integral de los puntos fuertes y débiles de la organización como un todo. Debe buscarse por esta vía una mayor integración para que todos reconozcan que el ambiente es el mismo y que las diferencias no son más que perspectivas personales al mirar el mismo terreno (Referencia: Introducción al procesamiento de datos del autor.).

La reorganización con un estilo abierto de participación permite eliminar brechas y descubrir el camino hacia la utilización de la computadora como una herramienta.

Con esta óptica, se podrían hacer ajustes organizativos sin limitar la motivación de las personas que están vinculadas directa o indirectamente con los sistemas, ya sea por haberlos desarrollado inicialmente o por ser sus usuarios más importantes. En esta primera etapa, deberían individualizarse las áreas claves de toda la organización y de su CPD en particular para concentrarse en ellas. Como producto derivado de este estudio, debería poder responderse a preguntas como:

¿Cuáles son los objetivos de esas áreas claves, incluyendo el CPD?

¿Qué limitaciones en los sistemas de control nos impiden o dificultan alcanzarlos?

¿Cómo puedo utilizar la organización y el personal del CPD para superar estas limitaciones?

¿Cómo puedo utilizar la computadora para ayudar a las personas a superar esas limitaciones?

Un primer resultado práctico de esta etapa es lograr que el personal se sienta parte activa y responsable de la implantación de cambios y un segundo resultado práctico es la generación de una lista de todos los recursos críticos de la instalación (hardware, software, materiales, personal y sistemas de información) con vistas a encarar la segunda etapa. La clave es entonces aportar conocimientos sobre el tema que con el adecuado incentivo se reflejan en ideas concretas que surjan naturalmente desde dentro sin que resulten impuestas. Esto, por supuesto, no implica que el trabajo del

asesor sea totalmente pasivo, sino que actua como un catalizador para acelerar las reacciones que buscan mejorar la organización.

Este es el principio para iniciar el cambio. Buscar IDEAS RENOVADORAS que, con el apoyo de la organización, se podrán convertir en proyectos y éstos luego en realidades.

ETAPA 2 SEGURIDAD

Obviamente, el ciclo de capacitación no termina en los conocimientos básicos impartidos inicialmente. Luego del incapié inicial en la identificación general de componentes en una unidad, el énfasis debe trasladarse a los aspectos vinculados a la CONTINUIDAD DEL SERVICIO. Esto se traduce, en primera instancia, en un análisis de los dispositivos de seguridad que tiene el sistema.

La organización debe evaluar los recursos y los incidentes potenciales para cuantificar los riesgos y hacer un dictamen de la situación. Para encarar este trabajo es sumamente práctico disponer de una lista general de control. (Referencia: 42 Suggestions for Improving Security in Data Processing Operations IBM)

Además, debe tenerse en cuenta que el estudio será más sencillo si se dispone de un inventario actualizado de recursos de la instalación. Así pues la tarea de realizar un inventario o bien actualizar uno existente es una piedra funadmaental para construir un sistema de control. (No se puede controlar lo que se desconoce). Ahora bien, esta tarea no debe realizarse a ultranza; incluyendo cualquier producto que se encuentre, ya que de ese inventario general, no todos los recursos tienen el mismo valor. Pensando en ello, pueden seleccionarse recursos sensitivos (aquellos cuya pérdida o destrucción causa un daño material importante a la organización (afectando incluso su situación patrimonial) tratarlos especialmente, como forma inicial de reducir la cantidad de elementos a considerar.

Ese tratamiento inicial incluye detalles de quien administra cada recurso sensitivo (PROPIETARIO), como lo hace (PROCEDIMIENTO), quien accede (USUARIO) y desde donde (LUGAR).

Además, es importante disponer de una historia de los resultados de la gestión hasta el presente. A partir de estos datos se verificarán los incidentes realmente ocurridos y aquellos que puedan ocurrir.
El problema es cómo determinar aquellos que potencialmente pueden ocurrir. Como posibles guías se pueden considerar las

exposiciones a las que se ven enfrentados genéricamente los servicios informáticos o más particularmente aquellos con marcadas semejanzas con el que está siendo ajustado.

Con esta óptica podemos considerar inicialmente la siguiente lista:

1) Falla en los equipos y los programas (destrucción de pistas en un disco, cintas magnéticoas averiadas, procesador fuera de servicio, errores de programación que dañan archivos).

2) Utilización maliciosa o criminal de los recursos (sabotaje, operación malintencionada del computador, espionaje industrial, extorsión).

3) Invasión de privacidad (obtención indebida de información con propósitos políticos, económicos o simple curiosidad).

4) Catástrofes (incendios, inundaciones, guerra, etc.)

La medida de la importancia de cada categoría para una organización en particular sólo puede darla la propia organización.

Difícilmente en un libro se encuentra una receta para encarar semejante tarea. Sin perjuicio de ello, no está demás estudiar los planteamientos hechos por otros, especialmente si existen variados ejemplos de situaciones reales que puedan asimilarse a las propias.

Este esfuerzo inicial debe idientificar aquellos incidentes que pueden ocurrir en la organización ya que nadie está prevenido de lo que desconoce.

(Referencia: Security Accuracy and Privacy in Computer Systems James Martin es el planteo inicial y ejemplos)

Una vez identificados los incidentes potenciales, deben analizarse los costos operativos de los mecanismos de prevención o protección y compararlos contra los riesgos derivados de los controles no implementados. Debe verificarse concretamente si el costo de la protección del recurso no es superior al costo de los percances derivados de la falta o insuficiencia de procedimientos de seguridad.

Para hacer la comparación, hay que estudiar el impacto que tienen los incidentes sobre el servicio, por ejemplo, imposibilidad de procesar, pérdida de información o bien invasión de privacidad por copia o acceso no autorizado.

Ahora bien, estos planteamientos no son más que herramientas auxiliares para determinar la real situación de una organización en caso general, pero volviendo al punto inicial, el problema de como encarar la seguridad en un sistema de procesamiento de datos, es más complejo que puntear una lista de posibles controles y sus ponderaciones relativas.

Una posible alternativa puede encontrarse en el desarrollo de un plan integral de revisión del aspecto seguridad en una instalación. Al respecto, el siguiente planteo en etapas podría ser una posible solución:

1) Definir la filosofía que aplicará la organización respecto de todos sus sistemas de protección.

2) Establecer el valor real que la organización dará a determinados recursos que deben protegerse.

3) Definir un presupuesto para seguridad.

4) Delimitar responsabilidades y definir procedimientos de control.

5) Poner en práctica los procedimientos.

La idea de este plan es que la dirección superior defina la escala de valores de la organización con respecto a los riesgos potenciales que se le plantean. Recién allí tendrá sentido el estudio técnico y a partir de él las recomendaciones que se efectúen.

Para lograr este objetivo debe enfrentarse al personal superior con las carencias que tiene su organización. Con ese objetivo, se puede hacer una encuesta de opinión para que quede determinada la situación del área bajo su supervisión en los aspecto vinculados al tema. Como paso siguiente y mediante entrevistas personales se puede enfrentar al gerente con los riesgos potenciales de los que él es responsable y que de acuerdo con la encuesta no ha asumido. Estas charlas pueden ser el punto de partida de una toma de posición gerencial ante el tema. (Referencia: The considerations of Physical Security in a Computer Environment IBM, ver Auditing the Security System).
Si el plan tiene éxito, definir objetivos es más fácil pues puede surgir del concenso de los interesados y tener un sentido global que alcance toda la instalación.

Esto último es importante pues debe tenerse en cuenta que los riesgos no pueden evaluarse independientemente. La protección

de un componente en desmedro de otro da la misma garantía que el eslabón más flojo de una cadena a la tensión que la misma puede soportar sin romperse. Por ejemplo una empresa que tiene sistemas de resguardo contra accesos no autorizados, incendios, cortes de energía, fallas prolongadas en los equipos pero resulta que se le inunda el centro de cómputos que está en el subsuelo por un problema de desagüe ante una lluvia muy intensa ¿se puede decir que es un ejemplo de perfección?

A partir de una definición adecuada de los recursos que deben protegerse y de una estimación de su valor, es mucho más sencillo distribuir la asignación de un presupuesto dado.

Obviamente, como en otros temas, el monto adjudicado al rubro seguridad es un problema de política de la empresa pero con la salvedad de que si se dispone de información pormenorizada de la situación de todos los bienes informáticos, se puede resolver el problema con mayor razón de causa.

Finalmente, ese estudio debe concluir con un informe sobre el nivel de seguridad actual y recomendaciones a corto, mediano y largo plazo, brindando estimaciones de costo-beneficio de la solución recomendada y sus alternativas. Si el plan tiene éxito, la implantación será más sencilla, pues contará con apoyo del nivel superior.

Obviamente, esto no garantiza su éxito final, resta "vender" la solución a todos los niveles para lo cual los detalles operativos deberán ser ajustados de manera que no se choque innecesariamente con el personal encargado de poner en práctica las medidas recomendadas.

ETAPA 3 CONTROL

El control del nivel de servicio y los costos operativos de una instalación surge como requerimiento adicional, una vez que existen ciertas garantías sobre la continuidad del servicio. Después de que las cosas "salen" es natural que se desee que "salgan bien" y a "costo mínimo".

La idea de un servicio "bien" prestado está vinculada con las expectativas del usuario respecto del mismo. Por tal motivo el nivel de servicio debe definirse en coordinación con los usuarios de los sistemas.

A su vez, estos niveles de servicio deben expresarse en términos tales que sea sencillo evaluar su cumplimiento. Algunos indicadores pueden ser los tiempos de respuesta máximos admitidos para una determinada transacción medidos en segundos,

los tiempos diarios de disponibilidad del servicio medidos en horas, las garantías de utilización medidos en porcentajes y con interrupciones máximas que serán admitidas medidas en unidades de tiempo.

Por ejemplo, para la transacción depósito en caja de ahorro, el tiempo de respuesta máximo será de 5 segundos. El servicio estará disponible durante todo el horario bancario y dos horas adicionales después del cierre. Podrá utilizarse respectivamente el servicio el 95% del tiempo de disponibilidad estimada y en ningún caso las interrupciones por problemas en casa matriz serán mayores de 3 horas. Para estos casos excepcionales de interrupción se dispondrá de un sistema local en cada dependencia y se bloquearán los movimientos cruzados entre dependencias.

Un buen punto de partida para establecer niveles de servicio es definir con precisión que utilizar para medir el servicio. Para ello es útil definir que se entiende por: disponibilidad, capacidad, rendimiento y confiabilidad.
Disponibilidad: es el tiempo en que el servicio está operativo.
Capacidad: es una medida de volumen de trabajo máximo que puede ser procesado en un tiempo fijo.
Rendimiento: es una medida de volumen de trabajo que es procesado en un tiempo fijo.
Confiabilidad: es la posibilidad de utilizar los recursos con la disponibilidad, capacidad y rendimiento establecidos.

Surge entonces una interrogante: ¿cómo medir esos factores en un sistema de procesamiento de datos?

Algunos indicadores para evaluar cada uno de los factores anteriores pueden ser;

DISPONIBILIDAD	Porcentajes absolutos
	Distribución en el tiempo
	Estadísticas de tipos de incidente
	Tiempos promedio de resolución de problemas
CAPACIDAD	Cantidades de instrucciones por segundo
	Velocidades de transferencia entre dispositivos de la configuración
	Velocidad en líneas de trasmisión
	Líneas por minuto
	Transacciones por segundo
	Trabajos por hora
	Traducciones por día
RENDIMIENTO	Tiempo de respuesta por transacción
	Porcentajes de utilización de los recursos
	Distribución de uso de los recursos

Programas modificados por unidad de tiempo/programador
Lineas de programas desarrollados por unidad de tiempo/programador

CONFIABILIDAD Encuestas
Información histórica

Además, la confiabilidad puede medirse sobre la base de indicadores que vinculen datos obtenidos indirectamente de DISPONIBILIDAD, CAPACIDAD y RENDIMIENTO, como ser:

- Disponibilidad durante una jornada completa
- Tiempo entre incidentes
- Duración de incidentes
- Distribución de los tiempos de respuesta en un lapso de tiempo dado.

Estos elementos pueden servir de referencia para cuantificar la situación de una instalación. A su vez, permiten obtener indicadores de utilización de los recursos.

El problema una vez identificados los niveles es cómo controlar su cumplimiento y su costo.

El eje es el control de actividades de producción y desarrollo y su comparación contra los estandares de la instalación o, más genéricamente, del mercado en ambientes similares. Un punto de partida para contralor de actividades es la obtención de reportes apropiados como subproducto de la bitácora de consola, de los sistemas de contabilidad automática o de herramientas de medición de performance.

Estos estudios permiten incluso estimar costos operativos por ambiente y más detalladamente por usuario llegando incluso a controlar la gestión de los especialistas dentro del CPD.

Adicionalmente, también es útil disponer de información de operaciones como ser: libro de incidentes conteniendo causa del incidente, fecha de apertura, fecha de cierre y solución adoptada; libro de quejas de los usuarios; libro de datos entrados y re-ortes distribuídos, conteniendo fecha, hora y descripción del envío; consumo de suministros (especialmente papel y cintas de impresora, para conformar resultados de calidad del servicio obtenido por otras vías (Referencia: Casos prácticos para estudio de Auditoría de Sistemas del autor).

Con respecto al área de desarrollo existen indicadores de productividad que se pueden extraer indirectamente del sistema de contabilidad aunque, hoy por hoy, es prácticamente

insustituible una metodología de desarrollo y control interno de aplicaciones que apunte a medir más la calidad que la cantidad de trabajo (Referencia: Programming Real-time Computer Systems, James Martin)

O ro aspecto importante es el vinculado con las tareas de mantenimiento de la instalación o, más genéricamente, con la determinación y resolución de problemas derivados de cambios.

La determinación de problemas es una especialidad; los procedimientos en el manejo de la determinación de problemas han dejado de ser un asunto que se pueda controlar empíricamente para dar lugar a un tratamiento científico, lo que exige una formulación teórica adecuada y muchos conocimientos té nicos (Referencia: El control de la gestión de cambios del autor).

ETAPA 4 PLANIFICACION

A medida que las organizaciones se van haciendo más grandes y complejas van perdiendo flexibilidad y deben soportar una mayor inercia ante los cambios. Con los vehículos sucede algo similar; es más fácil manejar un pequeño auto que un camión de 10 toneladas; a su vez, detenerlo, ponerlo en marcha o doblar implicará mayor o menor dificultad de acuerdo al peso y características de la carga. El problema no es solo la pericia del conductor (la dirección), también influye el estado de la carretera (ambiente), el acompañante (asesoramiento) y la hoja de ruta (planificación) en otros factores. Este último elemento es importante pues, sin una buena hoja de ruta no se puede preparar el vehículo con suficiente antelación para enfrentar los peligros de la carretera, lo que aumenta el riesgo de accidentes a la vez que obliga a reducir el régimen de marcha.

¿Cómo combatir los problemas derivados de la administración de organizaciones muy grandes?
Una respuesta, sin duda, es: Planificar a largo plazo. Ahora bien, inmediatamente surge la pregunta.
¿Cómo planificar a largo plazo?
Primero hay que tener definidas políticas a nivel superior, en base a estas políticas establecer objetivos y en concordancia con ellos, planes a mediano plazo.
Es como levantar un edificio en el que en cada piso se asienta en el inferior y todos ellos en los cimientos con la diferencia de que se lo contruye de arriba para abajo.

Incluso hay quienes afirman que todavía hay un nivel más alto, los "dogmas" que le dan continuidad a una organización por generaciones (Referencia: Una Empresa y sus Credos, WATSON Jr.).

El problema es como construir ese edificio.

El principio es el mismo que en cualquier actividad: involucrar el nivel superior, a aquel que dirige y toma las decisiones más importantes. Con este criterio, el primer reto es integrar a la Administración Superior en grupos de trabajo interdiciplinarios para la definición de los grandes sistemas de información que apoyan a la organización para alcanzar las metas políticas que ésta se ha propuesto.

Habrá que trabajar luego en la definición práctica de los objetivos fundamentales de cada área funcional, identificando problemas de carácter general y definiendo planes concretos para corregirlos. Recién en este punto se deberá pensar en los problemas técnicos derivados de la mecanización de los sistemas y los recursos para emprender su implementación por computadora. Luego los recursos financieros definirán la estrategia o seguir para la mecanización de los sistemas.

Sin embargo, este punto es crítico ya que en esta etapa pueden perderse de vista los objetivos de la organización al ser "sustituídos" por los objetivos del propio CPD que suelen estar en manos de especialistas sin que se arbitre ningún sistema de control que rectifique posibles desviaciones.

Por sobre todo no debe olvidarse que la informática es un recurso que, aunque muy versátil, no tiene un fin por si mismo sino que es un medio para operar, controlar y decidir en una organización.

Una herramienta sumamente útil para controlar la gestión y para asegurar que los planes se ajusten a las necesidades de la organizacion y que puestos en marcha se cumplan es la DIRECCION POR OBJETIVOS (DIPO) que aplicado al área informática garantiza como beneficio adicional una visión más global de los problemas de una empresa.

Además, el ciclo de la DIPO ayuda a controlar la gestión ya que no solamente permite detectar áreas claves definiendo objetivos para cada uno de ellas sino que orienta para establecer planes de acción concordantes con dichos objetivos y "obliga" a establecer puntos de control para evaluar resultados y retroalimentar el sistema evitando grandes desviaciones (Referencia: Curso de Introducción a las técnicas DIPO de J. Antonelli).

CONCLUSIONES

Los controles deben abarcar todos los componentes del sistema. Esto es personal, equipos, materiales y procedimientos que son

utilizados en el ciclo de elaboración de la información. A su vez, debe existir cierto equilibrio que no deje abiertos flancos de mayor exposición por haber concentrado los controles sobre un área en desmedro de otra. En la medida en que los controles deben ser aceptados como soluciones a los problemas planteados, su introducción debería surgir naturalmente y ser apoyada desde el seno de la organización. Para lograrlo de la misma manera que un bebé comienza gateando para luego caminar a los tropezones y, por último, aprender a caminar correctamente e incluso a correr, la implementación de sistemas de control interno requiere un proceso de concepción y desarrollo para luego alcanzar la madurez y por que no, en algunos casos acogerse a la "jubilación" cuando ya no esten en condiciones de rendir los frutos que en otra etapa brindaron.

Los problemas más difíciles de resolver al implantar un sistema de control interno, no son los estrictamente técnicos. El talón de Aquiles en la estrategia de implantación es ganar la colaboración del personal. Debe buscarse entonces un procedimiento por el cual el personal de Dirección y sus subordinados identifiquen objetivos comunes, definan áreas de responsabilidades de cada persona de acuerdo con los resultados que se esperan de su trabajo y utilicen esos resultados para medir la contribución de cada uno de sus empleados al cumplimiento de los objetivos corporativos.

De esta manera, podrá encaminarse la fuerza individual de cada persona, será más fácil establecer formas de trabajo grupales y podrá armonizarse las metas individuales con el fin común.

No debe olvidarse que la real dificultad al impulsar nuevos sistemas de control se encuentra en el espacio interior, ese que todo hombre tiene entre oreja y oreja y que requiere tiempo para ser modificado. Además, en ese espacio es difícil imponer cambios; hay que lograr que sean aceptados y para ello hay que estar dispuestos a actuar con flexibilidad para luego recoger los frutos del esfuerzo.